



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/808,709

03/16/2004

Richard J. Kuehnel

KUEHNEL 3-1

5945

27973 7590 09/28/2007

OFFICE OF THE ASSOC. GEN. COUNSEL (IP & T)
9800 SAVAGE ROAD
SUITE 6542
FORT MEADE, MD 20755-6542

EXAMINER

YAARY, MICHAEL D

ART UNIT

PAPER NUMBER

2193

MAIL DATE

DELIVERY MODE

09/28/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/808,709	Applicant(s) KUEHNEL ET AL.	
	Examiner Michael Yaary	Art Unit 2193	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07/05/2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-4 are pending in the application.

Response to Arguments

2. Applicant argues in the remarks, in response to the previous 101 rejection, that the claims do not preempt every substantial practical application of the idea that is embodied in the claims; that the claims are not so broad and sweeping as to cover both known and unknown uses of a pseudo-random bit sequence; and that the claims are already specific as to the implementation of the claims.

3. Examiner respectfully disagrees with applicant's remarks. It is in fact the statutory subject matter claimed, the device and method, which preempts every substantial practical application. As the claims are directed to the structure and method of generating a pseudo-random bit sequence, however not disclosing in what environment the claimed invention is utilized. Thus, preempting every possible use for a pseudo-random bit sequence and making the claimed invention so broad and sweeping as to cover all known and unknown uses of a pseudo-random bit sequence. Applicant asserts that the current claims are already specific as to what components make up the device, steps to the method and their use. However, the claim limitations disclose

otherwise, as they are directed to "generating an uncorrelated pseudo-random bit sequence uniformly distributed over a user-definable value K, where K+1 has m prime factors," thus not alleviating the fact that this is so broad and sweeping as to cover all known and unknown uses of a pseudo-random bit sequence. By amending the claims as to include, as taught by the specification, the environment or implementation of the claimed invention, the preemption would be overcome.

4. Applicant's arguments, filed 07/05/2007, with respect to the rejection(s) of claim(s) 3 and 4 under 35 U.S.C. 102(b) have been fully considered and are persuasive. Therefore, the previous rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1-4 are rejected under 35 U.S.C. 101 as the claims are directed to non-statutory subject matter.

(i) As to claims 1 and 3, the claims appear to preempt every substantial practical application of the idea that is embodied by the claims. The patent sought is on a method and device for generating an uncorrelated pseudo-random bit sequence. Sets forth in

the present claims are a generalized structure and way of determining an uncorrelated pseudo-random bit sequence. The device and method are so broad and sweeping as to cover both known and unknown uses of a pseudo-random bit sequence and the end result may vary greatly as to be used in various application types, thus covering both known and unknown uses of the pseudo-random bit sequence. Suggested ways to overcome the rejection would be to incorporate into the claims, as taught by the specification, specific implementation of which the claimed invention may be used for. An example would be as provided in the specification on page 5, lines 6-12 where pseudo-random number generation is provided for a cryptographical system.

(ii) Claims 2 and 4 are rejected for similar reasons as discussed for their respective parent claims, as they fail to present any limitations that resolve the deficiencies of the claims from which they depend.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mullen et al. (hereafter Mullen)(US Pat. 5,446,683) in view of Brandman (US Pat. 5,974,144).

9. **As to claim 3**, Mullen discloses a method of generating an uncorrelated pseudo-random bit sequence (abstract), comprising the steps of:

Generating m pseudo-random sequences (Abstract and column 3, lines 24-45 disclose generating a plurality of bit sequences), r_1, r_2, \dots, r_m , and generating the uncorrelated pseudo-random sequence (Column 3, lines 24-45 disclose generating the pseudo-random sequence based on the plurality of bit sequences.).

10. Mullen does not disclose selecting a user-definable value K , where K is a positive integer; factoring $K+1$ into M prime factors q_1, q_2, \dots, q_m); where each pseudo-random bit sequence r_i is uniformly distributed over a range $(0, \dots, q_i-1)$ where $i = 1, 2, \dots, m$; and the uncorrelated pseudo-random sequence is $R = r_1 + q_1 r_2 + q_1 q_2 r_3 + q_1 q_2 \dots q_{m-1} r_m$.

11. However, Brandman discloses selecting a user-definable value K , where K is a positive integer; factoring $K+1$ into M prime factors q_1, q_2, \dots, q_m); where each pseudo-random bit sequence r_i is uniformly distributed over a range $(0, \dots, q_i-1)$ where $i = 1, 2, \dots, m$; and the uncorrelated pseudo-random sequence is $R = r_1 + q_1 r_2 + q_1 q_2 r_3 + q_1 q_2 \dots q_{m-1} r_m$ (Abstract and column 8, lines 23-50 disclose in a cryptographic system, a security technique utilizing prime factorization. Furthermore, the numbers or constants should have large prime numbers to provide a strong cryptographic system. Brandman does not explicitly disclose utilizing the prime factors in the uncorrelated pseudo-random sequence $R = r_1 + q_1 r_2 + q_1 q_2 r_3 + q_1 q_2 \dots q_{m-1} r_m$, however, it would have been

Art Unit: 2193

obvious to one of ordinary skill in the art to incorporate the prime factors in to the sequence or a similar one to achieve the same predicted result.).

12. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Mullen, by incorporating the use of prime factors and prime factorization in a cryptographic system, as taught by Brandman, for the benefit of achieving a level of security in a pseudo-random sequence environment such as one used in the areas of encryption and cryptography.

13. **As to claim 4**, the combination of Mullen and Brandman does not explicitly disclose that q_1, q_2, \dots, q_m are ordered from smallest value q_1 to largest value q_m . However, examiner is taking official notice that it would have been obvious to one of ordinary skill in the art at the time of the invention to manipulate the factors in this or similar way in order to achieve the predicted result of an uncorrelated pseudo-random sequence.

Allowable Subject Matter

14. Claims 1 and 2 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 101 set forth in this Office action.

Art Unit: 2193

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Yaary whose telephone number is (571) 270-1249. The examiner can normally be reached on Monday-Friday, 8:00 a.m - 5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Meng-Ai An can be reached on (571) 272-3756. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MY

MY



MENG-AL T. AN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100